REMARKS

Pending Claims

In this application, claims 1-14, and 41-47 are currently pending. Claims 15-40 were previously withdrawn in response to a restriction requirement. Claims 1 and 12 have been amended by this Response. Claims 2-11, 13, and 14 have not be altered since filing. Claims 41-47 have been added. Entry of these amendments is respectfully requested.

Rejections under §101

Claims 1-11 were rejected under §101 as being non-statutory subject matter. In response, the word "electronically" has been added to the preamble of claim 1 as well as steps b) and d). Furthermore, several elements in amended claim 1 have been described as being stored on a user computer. These amendments should overcome the §101 rejection.

Rejections under §§102 and 103

Claim 1 was also rejected under §102(e) as being anticipated by Colosso (U.S. Patent 6,169,976). Colosso teaches a system for ensuring that software is properly licensed to a particular user. In Colosso, a central licensor creates a unique serial number every time the software distributor informs the licensor about a sale to a customer. Colosso, col. 3, lines 1-14. The created serial number is stored in a central database along with a user ID that is generated for the identified customer. Colosso, col. 11, lines 49-67. The serial number is then sent to both the distributor and the customer. Colosso, col. 12, lines 19-48. Only at this point does the customer receive the software, still in its encrypted form. Colosso, col. 12, lines 49-57. To activate the software, the customer submits its user ID and the software's serial number to the licensor, which compares this information to the data in the central database. Colosso, col. 13, lines 7-59. If the database confirms that this unique serial number has been associated with the supplied user ID, the Licensor supplies the customer with the installation and activation key necessary to use the software. Colosso, col. 13, lines 60-64; col. 14, lines 56-64; and col. 15, lines 19-25.

In contrast, claim 1 requires four separate steps to verify that a user is licensed to access digital content within a content file, none of which are found in Colosso:

a) obtaining a product ID from the content file stored on a user computer, the content file containing the digital content;
b) electronically comparing the product ID from the content file with a second product ID found in a product license stored on the user computer;
c) obtaining a first user ID from the product license; and
d) electronically comparing the first user ID from the product license with a second user ID found in a user license stored on the user computer.

As for step a), the Office Action states that the "content file" corresponds to the central database 314 of Colosso in Fig. 3, with the product ID corresponding to the serial number. However, step a) now requires that the content file be stored on the user computer, and that the content file contain the digital content. The central database 314 meets neither of these claim limitations. This distinction is crucial for the usefulness of the present invention, since the present invention has no need to look outside the digital content file to identify the product during license verification. The Colosso process of going to a centralized database to receive a serial number for the product requires, by necessity, a networked database that is constantly accessible to provide users with serial numbers after product purchases. This distinction alone is sufficient for claim 1 to be considered patentable over the Colosso reference.

The office action found that step b) was anticipated by the process Colosso, citing col. 11 lines 58—67, col. 13 lines 54—59, and col. 14 lines 15—30. These cited sections disclose the generation of the serial number, the storing of the serial number in the database, the activation request made by the customer, the comparison of the serial number and customer ID entered by the customer to the contents of the database, and the returning of key information to allow the customer to activate the software. In contrast, step b) of claim 1 compares the product ID from the content file with a second product ID found in a product license stored on the user computer. Thus, the claimed invention compares product IDs stored in two separate digital constructs on a local user computer, while Colosso matches a serial number manually entered by a user with a remotely located database. This distinction is again essential to obtain the benefits of the present invention—there is no need to access a remote database, and there is no need for user input.

Step c) of claim 1 ("obtaining a user ID from the product license") is said to be anticipated by Colosso (col. 14 lines 15—19). While the central database in Colosso contains a user ID, this user ID is not obtained from the product license that is stored on the user computer. As explained above, the ability to obtain this information from data constructs stored on the user computer greatly adds to the usefulness of the claimed invention.

Finally, step d) is not found in Colosso, which compares a user/login ID provided by a user with similar information in the database. Colosso, col. 13 lines 20—48. In contrast, step d) of claim 1 requires a comparison between a first user ID taken from the product license that is stored on the user computer with a second user ID that is found in a user license stored on the user computer. Thus, the two user IDs that are compared must be taken from two separate licenses, both of which must be found on the user computer.

In summary, Colosso does not teach or suggest any of the steps found in amended claim 1. The claimed steps define a unique invention that substantially improves on the technique used in Colosso. By verifying a license to access digital content using only a locally stored content file, product license, and user license, the present invention does not require network access, or user intervation. The steps from Colosso that the Office Action says are analogous might, depending on Internet connections and availability of the remote server and database, take hours.

Claims 2—11 depend from claim 1, and hence are allowable.

Claim 12 has been amended to clarify that the digital content file, the product license, and the user license are all structural elements stored on the computer that the user is on. For the reasons discussed in connection with claim 1, our invention is clearly distinguishable from the Colosso approach. Claims 13 and 14 depend from claim 12, and are therefore allowable.

New Claims:

Claims 41-47 are new claims relating to systems containing the product, product license, and user license described in the pending method claims. These claims are supported by the Specification as originally filed and are within the scope of the elected invention.

Related Application and Additional Prior Art:

The Applicant directs the Examiner's attention to pending U.S. Patent Application No. 09/845,041, now being examined by Examiner Daniel L. Greene in art unit 3621. This application owned by the assignee of the present application, has inventors in common with the present application, and is directed to a related invention. In this related application, Examiner Greene has emphasized Spagna, U.S. Patent no. 6,587,837; Peinado, U.S. Patent No. 6,775,655; and Colosso. The Spagna and Peinado references are included among the references listed in the supplemental IDS filed along with this response.

Spagna teaches a system for licensing digital content. As acknowledged by Examiner Greene in the related application, Spagna does not teach a product license that has a user identifier, a product identifier, and a decryption key; nor does Spagna teach a user license having a user identifier. Consequently, the claims of the present invention should be seen as patentable over Spagna, since all of the pending claims claims require a product license having a product ID and a user ID, and a user license having a user ID.

Peinado teaches a system where digital content is encrypted and provided with a product ID, and where a product license is provided that contains the product ID and the decryption code for the digital content. Peinado ties the product license to a particular user computer through a digital rights management (DRM) system that uses a "black box," as described in the summary of the invention:

> To implement `trust`, the DRM system is equipped with a `black box` that performs decryption and encryption functions for such DRM system. The black box includes a public/private key pair, a version number and a unique signature, all as provided by an approved certifying authority. The public key is made available to the license server for purposes of encrypting portions of the issued license, thereby binding such license to such black box. The private key is available to the black box only, and not to the user or anyone else, for purposes of decrypting information encrypted with the corresponding public key. The DRM system is initially provided with a black box with a public/private key pair, and the user is prompted to download from a black box server an updated secure black box when the user first requests a license. The black box server provides the updated black box, along with a unique public/private key pair. Such updated black box is written in unique executable code that will run only on the user's computing device, and is re-updated on a regular basis.
>
> When a user requests a license, the client machine sends the black box public key, version number, and signature to the license server, and such license server issues a license only if the version number is current and the signature is valid. A license request also includes an identification of the digital content for which a license is requested and a

> key ID that identifies the decryption key associated with the requested digital content. The license server uses the black box public key to encrypt the decryption key, and the decryption key to encrypt the license terms, then downloads the encrypted decryption key and encrypted license terms to the user's computing device along with a license signature.
>
> Once the downloaded license has been stored in the DRM system license store, the user can render the digital content according to the rights conferred by the license and specified in the license terms. When a request is made to render the digital content, the black box is caused to decrypt the decryption key and license terms, and a DRM system license evaluator evaluates such license terms. The black box decrypts the encrypted digital content only if the license evaluation results in a decision that the requestor is allowed to play such content. The decrypted content is provided to the rendering application for rendering.

Peinado, col. 3, lines 8-49. Thus, the digital content is encrypted and associated with a content identifier, while the product license has a matching product identifier and a key to decrypt the digital content. The key itself is encrypted using the black box public key, meaning only the black box with the secret private key can decrypt the key needed to decrypt the digital content. The black box itself is tied to the computer using "unique executable code that will run only on the user's computer device."

What is not found in Peinado (nor in any other prior art reference) is the unique system described in the pending claims, the system having a product license with a product ID and a user ID, and a user license having a user ID. Furthermore, many of the pending claims also require that the user license have a system ID that matches a system ID found on the computer system. The present invention has several significant advantages over the Peinado system, particularly in the method by which a license is verified. In Peinado, the link between the product license and a computer is a one-step process where a black box embedded into the operating system decodes the encryption key found in the product license. In contrast, the present invention takes two steps and does not require the black box system. Specifically, the product file is examined to discover a user ID, and the user ID is then used to find a user license stored on the computer. If the user license if found with the matching user ID, a system ID is taken from the user license and is matched against a system ID on the computer. In effect, the present invention replaced the black box of Peinado with a much simpler user license. The user license is not executable code, but merely a data construct that might take the form of an independent data file, or a registry or database entry. This system has several significant advantages over the system of Peinado. First, the required black box of

Peinado is an application program that must be run "in a protected or shrouded environment such that the user is denied access to such black box." Peinado, col. 15, lines 50-52. Consequently, this black box is operating system dependent, requires the creation of such a shrouded environment, is complex to create, and takes up a significant amount of space. In contrast, the user license of the present invention is a simple data construct that contains a user ID and a system ID. Since it is not an executable program, it does not require a special operating environment, it is operating system independent, it is simple to create, and occupies little storage space.

In addition, the black box of Peinado must be updated frequently to confound nefarious users, Peinado, col. 20, lines 7-35. This is because access to the black box application would effectively grant access to the digital content. The present invention does not update the user license, because the user license does not represent the same "weak link" as represented by the black box. While the black box is an application program that can be decompiled, analyzed, and broken, the user license is simply encrypted data. As such, the only method to break the user license is through brute force guessing, which is highly impractical using modern encryption techniques.

Finally, the Peinado system effectively locks a licensed product to a particular computer by encrypting the decryption key in the product license with the public key of the black box. The public/private key is assigned exclusively to a single black box, and the black box is written in unique executable code that will run only on the user's computing device. Peinado, col. 3, lines 13-26. Consequently, the product license is tied so closely with a particular computer that there is no ability to restore product licenses to a new computer due to computer malfunction or obsolescence. In contrast, the present invention's use of a user license allows licenses to be restored in a simple, but secured matter. This is explained in the Specification of the present application, paragraphs 0075-0078:

> Users 150 are authorized to transfer user licenses between machines a limited number of times. If the license is transferred without any interaction with the player software 152 or the license server 136, the transfer will be unsuccessful because a user license 160 is tied to a specific machine through the OS ID 162. If the license were merely moved without changing the embedded OS ID 162, there would not be a match in step 366, and the user license 160 would be ineffectual.
>
> To accomplish the transfer of user licenses 160, the player software 152 has the ability to save the license information to a safe location such as a floppy disk. If the hard disk

> containing the user license 160 then crashes, the user 150 can restore the user license 160 through the player software 152. To do so, the player software 152 requires the user 150 to enter the correct password 162. Then the player software 152 contacts the license server with request to recover a user license 152. This request would contain basically the same information sent to the license server 136 in step 464, including the new OS ID 162, as well as the User ID 156 that is being recovered. Assuming that user has not restored their user license 160 more than the pre-determined limit, the license server 136 will return a new user license 160 that will work with the new OS ID 162.
>
> The license server 136 keeps track of the number of times license restoration is attempted by a user 150. A limit is placed on how many times one can restore licenses from the license server 136. If credit card numbers are not always required to obtain a user license 160, then a lower limit for restorations can be placed on users 150 whose user license 160 does not contain credit cart information. Using this technique, it is possible to move a user license 160 to a different computer, albeit only limited number of times.
>
> If a hard drive is lost, not only is the user license 160 lost, but so also are all of the product license 154 that were on the drive. Consequently, player software 152 also allows a user 150 with a valid user license to query database 134 and download all known product licenses 154 for the user's user ID 160 that are not currently on the hard drive. In this way, a user can secure his or her licenses merely by backing up the user license to a floppy disk through the utility provided by player software 152. It is also possible in this manner to have a duplicate set of user license 160 and product licenses 154 on multiple computers.

Peinado simply cannot match this flexibility and security because it lacks the user license of the present invention.

This user license is integrated into the steps for independent method claims 1 and 12, and forms part of independent system claims 41 and 46. Consequently, all of the claims of the present invention are patentable over Peinado, Spagna, and the cited prior art. The Applicant respectfully submits that the claims are in condition for allowance.

CONCLUSION

All of the claims remaining in this application should now be seen to be in condition for allowance. The prompt issuance of a notice to that effect is solicited.

Respectfully submitted,
J. RIVER, INC.
By its attorneys:

Date: 30 March 2005

Daniel A. Tysver
Registration No. 35,726
Beck & Tysver, P.L.L.C.
2900 Thomas Ave., #100
Minneapolis, MN 55416
Telephone: (612) 915-9634
Fax: (612) 915-9637